Bridge CA Profile

The Federal Public Key Infrastructure Technical Working Group (FPKITWG) identified the need to profile the Bridge CA-certificate and cross-certificates issued between the BCA and other public key infrastructures. Subsequent discussions concluded that there is not an apparent need for a self-signed certificate for the self-issued Bridge CA key.

The extension profile for the cross certificates issued between the BCA and the various PKI infrastructures (Principal CAs – PCAs) is identified below.

The values used within this profile are defined below.

Required (r) – This field must be populated and processed.

Optional (o) – This field may be optionally populated or processed.

Critical (k) – If the extension is marked critical and is not recognized by the certificate processing application, the certificate must be rejected.

authorityKeyIdentifier Cross Certificate BCA to PCA	r	Required to build a certificate path.
authorityKeyIdentifier Cross Certificate PCA to BCA	r	Required to build a certificate path.
subjectKeyIdentifier Cross Certificate BCA to PCA	r	Required to build a certificate path.
subjectKeyIdentifier Cross Certificate PCA to BCA	r	Required to build a certificate path.
keyUsage Cross Certificate BCA to PCA	k,r	Limit public key usage to keyCertSign and cRLSign.
keyUsage Cross Certificate PCA to BCA	k,r	Limit public key usage to keyCertSign and cRLSign.
extendedKeyUsage Cross Certificate BCA to PCA	o	No other key usages defined.

extendedKeyUsage Cross Certificate PCA to BCA	o	No other key usages defined.
privateKeyUsagePeriod Cross Certificate BCA to PCA	o	No trusted time mechanism.
privateKeyUsagePeriod Cross Certificate PCA to BCA	o	No trusted time mechanism.
certificatePolicies Cross Certificate BCA to PCA	r	BCA must be able to specify policies in cross certificate. Set explicit policy indicator to "true."
certificatePolicies Cross Certificate PCA to BCA	o	A domain might not require this extension. Explicit policy indicator must be set to "False" if this extension is not present.
policyMappings Cross certificate BCA to PCA	o	Policy mappings are allowed, but not required.
policyMappings Cross Certificate PCA to BCA	o	Policy mappings are allowed, but not required.
subjectAltName Cross Certificate BCA to PCA	o	No subject alternate names used.
subjectAltName Cross Certificate PCA to BCA	o	No subject alternate names used.
issuerAltName Cross Certificate BCA to PCA	o	No issuer alternate names used.
issuerAltName Cross Certificate PCA to BCA	o	No issuer alternate names used.

subjectDirectoryAttribute Cross Certificate BCA to PCA	o	No directory attributes defined.
subjectDirectoryAttribute Cross Certificate PCA to BCA	o	No directory attributes defined.
basicConstraints Cross Certificate BCA to PCA	k,r	BCA must be able to issue cross certificates. Set CA Path Length to "optional."
basicConstraints Cross Certificate PCA to BCA	k,r	PCA must be able to issue cross certificates among other certificates.
nameConstraints Cross Certificate BCA to PCA	o	BCA may constrain the name space of a PCA, but it is not required.
nameConstraints Cross Certificate PCA to BCA	o	PCA shouldn't constrain the name space of the BCA.
policyConstraints Cross Certificate BCA to PCA	k,r	BCA must be able to constrain certificate policies. (Set initialPolicyMapping with SkipCerts = 0 and set requireExplicitPolicy).
policyConstraints Cross Certificate PCA to BCA	k,r	PCA must be able to constrain certificate policies. (Set initialPolicyMapping with SkipCerts ≤ 1 and do not set requireExplicitPolicy).
cRLDistributionPoints Cross Certificate BCA to PCA	o	The use of distribution points is not required.
cRLDistributionPoints Cross Certificate PCA to BCA	o	The use of distribution points is not required.